(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108476136 A
(43)申请公布日 2018.08.31

(21)申请号 201680078184.0

(22)申请日 2016.01.18

(85)PCT国际申请进入国家阶段日
2018.07.06

(86)PCT国际申请的申请数据
PCT/JP2016/051245 2016.01.18

(87)PCT国际申请的公布数据
WO2017/126001 JA 2017.07.27

(71)申请人 三菱电机株式会社
地址 日本东京都

(72)发明人 川合丰 平野贵人 小关义博

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 邓毅 马建军

(51)Int.Cl.
H04L 9/16(2006.01)
G09C 1/00(2006.01)

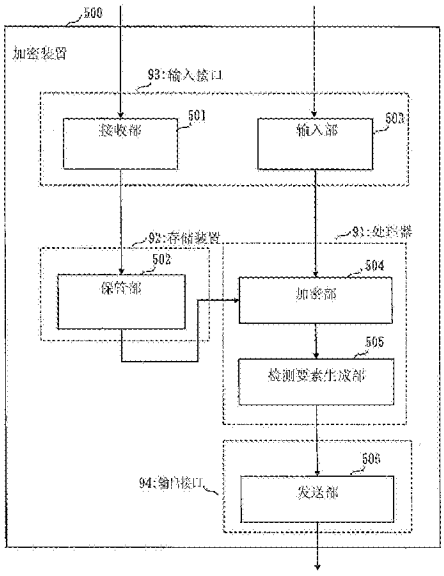
权利要求书2页 说明书12页 附图16页

(54)发明名称

加密装置、密文转换装置、加密程序、密文转换程序、加密方法和密文转换方法

(57)摘要

加密装置(500)具有加密部(504)、检测要素生成部(505)和发送部(506)。加密部(504)使用成对的2个密钥中的一个密钥对明文进行加密，由此，生成对明文进行加密后的能够进行同态运算的密文。检测要素生成部(505)使用一个密钥和密文，生成在密文的改变检测中使用的检测要素E。发送部(506)发送密文和检测要素。



CN 108476136 A

1.一种加密装置,其中,所述加密装置具有:

加密部,其使用成对的2个密钥中的一个密钥对明文M进行加密,由此,生成对所述明文M进行加密后的能够进行同态运算的密文D;

检测要素生成部,其使用所述一个密钥和所述密文D,生成在所述密文D的改变检测中使用的检测要素E;以及

输出部,其输出所述密文D和所述检测要素E。

2.根据权利要求1所述的加密装置,其中,

所述一个密钥是成对的第1公开密钥pk和第1秘密密钥sk中的所述第1公开密钥pk。

3.根据权利要求2所述的加密装置,其中,

所述加密装置具有保管部,该保管部保管共享参数pub,

所述加密部选择第1随机数r和第2随机数s,除了所述第1公开密钥pk以外,还使用所述第1随机数r和所述共享参数pub生成所述密文D,

除了所述第1公开密钥pk和所述密文D以外,所述检测要素生成部还使用所述第1随机数r、所述第2随机数s和所述共享参数pub生成所述检测要素E。

4.一种密文转换装置,其中,所述密文转换装置具有:

取得部,其取得对明文M进行加密后的能够进行同态运算的密文D和在所述密文D的改变检测中使用的检测要素E;

保管部,其保管有在向作为与所述密文D不同的密文的转换密文RC的转换中使用的转换密钥rk;

改变检测部,其根据所述检测要素E生成作为所述密文D是否被改变的基准的基准值,根据所述密文D生成在与所述基准值之间的核对中使用的核对值,进行所述基准值与所述核对值之间的核对;

转换部,其在所述改变检测部的核对结果为未检测到所述密文D的改变的情况下,通过使用所述转换密钥rk,将所述密文D转换成所述转换密文RC;以及

输出部,其输出所述转换密文RC。

5.根据权利要求4所述的密文转换装置,其中,

所述密文D是使用与第1秘密密钥sk成组的第1公开密钥pk对所述明文M进行加密而得到的,

使用所述第1公开密钥pk和所述密文D生成所述检测要素E,

根据与第2秘密密钥esk成对的第2公开密钥epk和所述第1秘密密钥sk,生成所述转换密钥rk,该第2秘密密钥esk是在对所述密文D实施了同态运算的情况下在同态运算的运算结果的解密中使用的解密密钥,

所述保管部保管所述第1公开密钥pk,

所述改变检测部根据所述检测要素E和所述第1公开密钥pk生成所述基准值,根据所述第1公开密钥pk和所述密文D生成所述核对值。

6.一种加密程序,其中,所述加密程序用于使计算机执行以下处理:

使用成对的2个密钥中的一个密钥对明文M进行加密,由此,生成对所述明文M进行加密后的能够进行同态运算的密文D;

使用所述一个密钥pk和所述密文D,生成在所述密文D的改变检测中使用的检测要素E;

以及

输出所述密文D和所述检测要素E。

7.一种密文转换程序，其中，所述密文转换程序用于使计算机执行以下处理：

取得对明文M进行加密后的能够进行同态运算的密文D和在所述密文D的改变检测中使用的检测要素E；

保管在向作为与所述密文D不同的密文的转换密文RC的转换中使用的转换密钥rk；

根据所述检测要素E生成作为所述密文D是否被改变的基准的基准值，根据所述密文D生成在与所述基准值之间的核对中使用的核对值，进行所述基准值与所述核对值之间的核对；

在核对结果为未检测到所述密文D的改变的情况下，通过使用所述转换密钥rk，将所述密文D转换成所述转换密文RC；以及

输出所述转换密文RC。

8.一种加密装置进行的加密方法，该加密装置具有加密部、检测要素生成部和输出部，其中，

所述加密部使用成对的2个密钥中的一个密钥对明文M进行加密，由此，生成对所述明文M进行加密后的能够进行同态运算的密文D，

所述检测要素生成部使用所述一个密钥pk和所述密文D，生成在所述密文D的改变检测中使用的检测要素E，

所述输出部输出所述密文D和所述检测要素E。

9.一种密文转换装置进行的密文转换方法，该密文转换装置具有取得部、保管部、改变检测部、转换部和输出部，其中，

所述取得部取得对明文M进行加密后的能够进行同态运算的密文D和在所述密文D的改变检测中使用的检测要素E，

所述保管部保管在向作为与所述密文D不同的密文的转换密文RC的转换中使用的转换密钥rk，

所述改变检测部根据所述检测要素E生成作为所述密文D是否被改变的基准的基准值，根据所述密文D生成在与所述基准值之间的核对中使用的核对值，进行所述基准值与所述核对值之间的核对，

所述转换部在所述改变检测部的核对结果为未检测到所述密文D的改变的情况下，通过使用所述转换密钥rk，将所述密文D转换成所述转换密文RC，

所述输出部输出所述转换密文RC。

加密装置、密文转换装置、加密程序、密文转换程序、加密方法和密文转换方法

技术领域

[0001] 本发明涉及同态加密。本发明涉及使用同态加密的加密装置、密文转换装置、加密程序、密文转换程序、加密方法和密文转换方法。

背景技术

[0002] 通常，当对数据进行加密后，如果不进行解密，则无法对内部的数据进行阅览和编集，因此，在对多个密文内的数据进行编集的情况下，需要进行一次解密而取出明文作为数据，然后进行编集，再次进行加密。与此相对，在同态加密中，能够在密文的状态下对内部的数据进行编集。此时的处理被称作同态运算，能够进行同态运算的种类、同态运算的次数根据具体方式而变化。

[0003] 作为同态加密，除了ElGamal加密和Pailier加密等仅能进行加法运算或仅能进行乘法运算的同态加密以外，还提出了能够无限制地执行加法运算和乘法运算的Gentry加密等。在这些方式中，存在如下课题：作为第一点，在进行同态运算时，必须利用相同的公开密钥生成密文；作为第二点，由于同态运算前的密文在加密后的状态下进行运算，因此，即使通过同态运算改变了明文也无法检测到。

[0004] 提出了若干针对这种课题的解决方式(例如参照专利文献1和非专利文献1)。

[0005] 现有技术文献

[0006] 专利文献

[0007] 专利文献1：国际公开第WO2014/010202A1号

[0008] 非专利文献

[0009] 非专利文献1：Keita Emura、Goichiro Hanaoka、Go Ohtake、Takahiro Matsuda、Shota Yamada：Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption.Public Key Cryptography 2013：32-50

发明内容

[0010] 发明要解决的课题

[0011] 在专利文献1记载的方法中，通过被称作代理重加密的技术，使利用多个不同密钥生成的密文变化成特定的一个密钥的密文，进行同态运算。

[0012] 但是，在该方法中，存在同态运算前的密文的安全性较低，明文数据能够改变这样的课题。

[0013] 在非专利文献1记载的其他方法中，代替在进行同态运算时需要特别的密钥，而提高同态运算前的密文的安全性的强度。具体而言，防止明文数据的篡改。

[0014] 但是，在该方法中，存在能够对同态运算后的密文进行解密的用户也能够对同态前的密文进行解密这样的课题。

[0015] 这样，在专利文献1、非专利文献1的情况下，同态运算前的密文的明文内容可能被

改变。

[0016] 因此，本发明的目的在于，提供检测同态运算前的密文的改变的装置、程序和方法。

[0017] 用于解决课题的手段

[0018] 本发明的加密装置的特征在于，所述加密装置具有：加密部，其使用成对的2个密钥中的一个密钥对明文M进行加密，由此，生成对所述明文M进行加密后的能够进行同态运算的密文D；检测要素生成部，其使用所述一个密钥和所述密文D，生成在所述密文D的改变检测中使用的检测要素E；以及输出部，其输出所述密文D和所述检测要素E。

[0019] 发明效果

[0020] 在本发明中，在对数据加密后的状态下能够进行数据运算的同态加密技术中，采用检测密文的改变的检测要素，因此，能够检测同态运算前的密文的改变。由此，能够实现使用未被改变的真正密文的、安全的同态运算的利用。

附图说明

[0021] 图1是实施方式1的图，是示出隐匿分析系统的结构的框图。

[0022] 图2是实施方式1的图，是共享参数生成装置的图。

[0023] 图3是实施方式1的图，是第1密钥生成装置的框图。

[0024] 图4是实施方式1的图，是第2密钥生成装置的图。

[0025] 图5是实施方式1的图，是加密装置的框图。

[0026] 图6是实施方式1的图，是转换密钥生成装置的框图。

[0027] 图7是实施方式1的图，是密文转换装置的图。

[0028] 图8是实施方式1的图，是同态运算装置的框图。

[0029] 图9是实施方式1的图，是第1解密装置的框图。

[0030] 图10是实施方式1的图，是第2解密装置所示的框图。

[0031] 图11是实施方式1的图，是示出共享参数生成装置的处理的流程图。

[0032] 图12是实施方式1的图，是示出第1密钥生成装置的处理的流程图。

[0033] 图13是实施方式1的图，是示出第2密钥生成装置的处理的流程图。

[0034] 图14是实施方式1的图，是示出加密装置的处理的流程图。

[0035] 图15是实施方式1的图，是示出转换密钥生成装置的处理的流程图。

[0036] 图16是实施方式1的图，是示出密文转换装置的处理的流程图。

[0037] 图17是实施方式1的图，是示出同态运算装置的处理的流程图。

[0038] 图18是实施方式1的图，是示出第1解密装置的处理的流程图。

[0039] 图19是实施方式1的图，是示出第2解密装置的处理的流程图。

[0040] 图20是实施方式1的图，是示出隐匿分析系统的数据的输入和输出的图。

[0041] 图21是实施方式1的图，是示出共享参数生成装置等的硬件结构的图。

[0042] 图22是实施方式1的图，是示出共享参数生成装置等的硬件结构的另一个图。

具体实施方式

[0043] 实施方式1

[0044] 下面，如下所述记载密钥生成装置300等。

[0045] (1)在实施方式1中，出现生成成对的公开密钥pk和解密密钥sk(秘密密钥)的密钥生成装置300。将该密钥生成装置300记作第1密钥生成装置300。

[0046] (2)将由第1密钥生成装置300生成的公开密钥pk、解密密钥sk记作第1公开密钥pk、第1解密密钥sk。另外，有时也记作公开密钥pk、解密密钥sk。

[0047] (3)在实施方式1中，出现生成成对的公开密钥epk和解密密钥esk(秘密密钥)的同态运算后密钥生成装置400。将该同态运算后密钥生成装置400记作第2密钥生成装置。

[0048] (4)将由第2密钥生成装置生成的公开密钥epk、解密密钥esk记作第2公开密钥epk、第2解密密钥esk。另外，有时也记作公开密钥epk、解密密钥esk。

[0049] (5)在实施方式1中，出现使用第1解密密钥sk对密文进行解密的解密装置900。将该解密装置900记作第1解密装置。

[0050] (6)在实施方式1中，出现使用第2解密密钥esk对同态运算后的密文进行解密的解密装置1000。将该解密装置1000记作第2解密装置。

[0051] 图1是示出隐匿分析系统100的结构的框图。如图1所示，隐匿分析系统100具有共享参数生成装置200、多个第1密钥生成装置300、多个第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000。

[0052] 在隐匿分析系统100中，共享参数生成装置200～第2解密装置1000也可以分别不经由互联网101连接，而是利用铺设于同一企业内的LAN(Local Area Network:局域网)连接来实现。

[0053] 互联网101是连接共享参数生成装置200、多个第1密钥生成装置300、多个第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000的通信路径。互联网101是网络的例子。也可以代替互联网101而使用其他种类的网络。

[0054] 共享参数生成装置200生成在系统中使用的共享的参数即共享参数pub，经由互联网101向多个第1密钥生成装置300、多个第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000发送共享参数pub。另外，也可以不经由互联网101而通过邮寄、网站的公告板等提供该共享参数pub。

[0055] 另外，在以下的加密装置500等的说明中，在没有共享参数pub的取得说明的情况下，设为已经取得该共享参数pub。

[0056] 第1密钥生成装置300可以是个人计算机。第1密钥生成装置300是如下计算机：生成公开密钥pk和解密密钥sk，向加密装置500、密文转换装置700和第1解密装置900发送公开密钥pk，向转换密钥生成装置600和第1解密装置900发送解密密钥sk。

[0057] 第2密钥生成装置400可以是个人计算机。第2密钥生成装置400是如下计算机：生成第2公开密钥epk和第2解密密钥esk，向转换密钥生成装置600和同态运算装置800发送第2公开密钥epk，向第2解密装置1000发送第2解密密钥esk。

[0058] 加密装置500作为数据的加密装置发挥功能，可以是个人计算机。加密装置500是如下计算机：从第1密钥生成装置300接收公开密钥pk，并且从外部输入明文M，输出密文C。

[0059] 转换密钥生成装置600可以是个人计算机。转换密钥生成装置600是如下计算机：从第1密钥生成装置300接收解密密钥sk，从第2密钥生成装置400接收第2公开密钥epk，生成转换密钥rk，并发送给密文转换装置700。

[0060] 密文转换装置700可以是个人计算机。密文转换装置700是如下计算机：从转换密钥生成装置600接收转换密钥rk，输入密文C，取得公开密钥pk，生成并输出对密文C进行转换后的转换密文RC。

[0061] 同态运算装置800可以是个人计算机。同态运算装置800是如下计算机：从第2密钥生成装置400接收第2公开密钥epk，输入多个转换密文RC，输出执行同态运算后的密文EC(以下为密文EC)。

[0062] 第1解密装置900可以是个人计算机。第1解密装置900是如下计算机：从第1密钥生成装置300接收解密密钥sk，取得公开密钥pk，输入密文C，输出密文C的解密结果。

[0063] 第2解密装置1000可以是个人计算机。第2解密装置1000是如下计算机：从第2密钥生成装置400接收第2解密密钥esk，输入密文EC，输出密文EC的解密结果。

[0064] 另外，也可以在同一个人计算机内同时包含第1密钥生成装置300、解密装置900、转换密钥生成装置600中的任意2个以上。

[0065] 另外，也可以在同一个人计算机内同时包含第2密钥生成装置400和第2解密装置1000。

[0066] 另外，也可以在同一个人计算机内同时包含转换密钥生成装置600、密文转换装置700、同态运算装置800中的任意2个以上。

[0067] <***结构的说明***>

[0068] 下面，对本实施方式的结构进行说明。

[0069] 如图1所示，隐匿分析系统100具有共享参数生成装置200、多个第1密钥生成装置300、多个第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000。

[0070] 图2～图10是示出装置均为计算机的共享参数生成装置200、第1密钥生成装置300、第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000的结构的框图。

[0071] 图21是示出共享参数生成装置200～第2解密装置1000的硬件结构的图。

[0072] 在本实施方式中，共享参数生成装置200、第1密钥生成装置300、第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000是计算机。

[0073] 共享参数生成装置200、第1密钥生成装置300、第2密钥生成装置400具有处理器91、输入接口93、输出接口94这样的硬件。加密装置500～第2解密装置1000具有处理器91、存储装置92、输入接口93、输出接口94这样的硬件。下面，输入接口93、输出接口94记作输入I/F93、输出I/F94。

[0074] 在图2～图10中示出各功能部与硬件的关系。在图2～图10中，作为处理器91示出的“～部”由软件实现。即，作为处理器91示出的“～部”通过处理器91执行软件来实现。并且，图5～图10中的“保管部”由存储装置92实现。

[0075] 处理器91经由信号线而与其它硬件连接，对这些其他硬件进行控制。处理器91是

进行处理的IC(Integrated Circuit:集成电路)。具体而言,处理器91是CPU(Central Processing Unit:中央处理单元)。

[0076] 存储装置92包含辅助存储装置92a和存储器92b。具体而言,辅助存储装置92a是ROM(Read Only Memory:只读存储器)、闪存或(Hard Disk Drive:硬盘驱动器)。具体而言,存储器92b是RAM(Random Access Memory:随机存取存储器)。

[0077] 输入I/F93是供信号输入的端口。并且,输入I/F93可以是与鼠标、键盘、触摸面板这样的输入装置连接的端口。具体而言,输入I/F93是USB(Universal Serial Bus:通用串行总线)端子。另外,输入接口93也可以是与LAN(Local Area Network:局域网)连接的端口。

[0078] 输出I/F94是输出信号的端口。输出I/F94可以是USB端子。

[0079] 在辅助存储装置92a中存储有实现作为处理器91示出的“～部”的功能的程序。该程序载入到存储器92b,读入到处理器91,由处理器91来执行。在辅助存储装置92a中还存储有OS(Operating System:操作系统)。OS的至少一部分载入到存储器92b,处理器91执行OS,并且执行实现作为处理器91示出的“～部”的功能的程序。

[0080] 共享参数生成装置200～第2解密装置1000可以仅具有一个处理器91,也可以具有多个处理器91。多个处理器91可以协作执行实现“部”的功能的程序。

[0081] 表示作为处理器91示出的“部”的功能的处理结果的信息、数据、信号值和变量值存储在辅助存储装置92a、存储器92b或处理器91内的寄存器或高速缓冲存储器中。

[0082] 实现作为处理器91示出的“部”的功能的程序也可以存储在磁盘、软盘、光盘、高密度盘、DVD(Digital Versatile Disc:数字多功能盘)这样的移动记录介质中。

[0083] 图2是示出共享参数生成装置200的结构的框图。如图2所示,共享参数生成装置200具有输入部201、共享参数生成部202和发送部203。虽然未图示,但是,共享参数生成装置200具有存储在共享参数生成装置200的各部中使用的数据的记录介质。输入部201输入在本系统中使用的密钥的比特长度L_{bit}。接着,共享参数生成部202生成作为在本系统中使用的运算基础的共享参数pub。虽然未图示,但是,为了生成共享参数pub,共享参数生成部202也可以具有随机数生成功能。发送部203向多个第1密钥生成装置300、多个第2密钥生成装置400、加密装置500、转换密钥生成装置600、密文转换装置700、同态运算装置800、第1解密装置900和第2解密装置1000发送由共享参数生成部202生成的共享参数pub。

[0084] 图3是示出第1密钥生成装置300的结构的框图。如图3所示,第1密钥生成装置300具有输入部301、密钥生成部302和密钥发送部303。虽然未图示,但是,第1密钥生成装置300具有存储在第1密钥生成装置300的各部中使用的数据的记录介质。输入部301输入共享参数pub。接着,密钥生成部302生成第1公开密钥pk与第1解密密钥sk的对。虽然未图示,但是,为了生成pk和sk,密钥生成部302也可以具有随机数生成功能。密钥发送部303向加密装置500、密文转换装置700和第1解密装置900发送由密钥生成部302生成的第1公开密钥pk,向转换密钥生成装置600和第1解密装置900发送所生成的第1解密密钥sk。

[0085] 图4是示出第2密钥生成装置400的结构的框图。如图4所示,第2密钥生成装置400具有输入部401、密钥生成部402和密钥发送部403。虽然未图示,但是,第2密钥生成装置400具有存储在第2密钥生成装置400的各部中使用的数据的记录介质。输入部401输入共享参数pub。密钥生成部402生成第2公开密钥epk与第2解密密钥esk的对。虽然未图示,但是,为

了生成第2公开密钥epk和第2解密密钥esk，密钥生成部402也可以具有随机数生成功能。密钥发送部403向转换密钥生成装置600和同态运算装置800发送由密钥生成部402生成的第2公开密钥epk，向第2密文解密装置1000发送所生成的第2解密密钥esk。

[0086] 图5是示出加密装置500的结构的框图。如图5所示，加密装置500具有接收部501、保管部502、输入部503、加密部504、检测要素生成部505和发送部506。虽然未图示，但是，加密装置500具有存储在加密装置500的各部中使用的数据的记录介质。接收部501输入第1公开密钥pk。保管部502保管第1公开密钥pk。输入部503从外部输入明文M。加密部504根据保管部502中保存的第1公开密钥pk和由输入部503输入的明文M生成密文D。虽然未图示，但是，为了生成密文D，加密部504也可以具有随机数生成功能。检测要素生成部505根据密文D和第1公开密钥pk生成检测要素E。虽然未图示，但是，为了生成检测要素E，检测要素生成部505也可以具有随机数生成功能。发送部506输出密文C＝(D、E)。即，发送部506输出密文D和检测要素E的组作为密文C。

[0087] 图6是示出转换密钥生成装置600的结构的框图。如图6所示，转换密钥生成装置600具有接收部601、保管部602、输入部603、转换密钥生成部604和发送部605。虽然未图示，但是，转换密钥生成装置600具有存储在转换密钥生成装置600的各部中使用的数据的记录介质。接收部601接收解密密钥sk。接着，保管部602保管解密密钥sk。输入部603输入第2公开密钥epk。转换密钥生成部604根据保管部602中保存的第1解密密钥sk和由输入部603输入的第2公开密钥epk生成转换密钥rk。

[0088] 即，rk＝RKG(epk、sk)。

[0089] RKG是表示转换密钥rk的生成的运算记号。虽然未图示，但是，为了生成转换密钥rk，转换密钥生成部604也可以具有随机数生成功能。发送部605向密文转换装置700发送转换密钥rk。

[0090] 图7是示出密文转换装置700的结构的框图。如图7所示，密文转换装置700具有接收部701、保管部702、输入部703、改变检测部704、密文转换部705和发送部706。虽然未图示，但是，密文转换装置700具有存储在密文转换装置700的各部中使用的数据的记录介质。

[0091] 接收部701接收转换密钥rk。保管部702保管转换密钥rk。对输入部703输入密文C＝(D、E)和第1公开密钥pk。改变检测部704使用第1公开密钥pk，验证由输入部703输入的密文C的明文M是否未被改变。密文转换部705根据保管部702中保存的转换密钥rk和由输入部703输入的密文C生成转换密文RC。在由改变检测部704检测到改变的情况下，作为转换密文RC，密文转换部705将表示改变的特殊记号代入转换密文RC中。在改变检测部704未检测到改变的情况下，生成转换密文RC。虽然未图示，但是，为了生成转换密文RC，密文转换部705也可以具有随机数生成功能。发送部706输出转换密文RC。

[0092] 图8是示出同态运算装置800的结构的框图。如图8所示，同态运算装置800具有接收部801、保管部802、输入部803、同态运算部804和发送部805。虽然未图示，但是，同态运算装置800具有存储在同态运算装置800的各部中使用的数据的记录介质。接收部801接收转换密文RC。保管部802保管多个由接收部801接收到的转换密文RC。输入部803输入第2公开密钥epk。同态运算部804根据保管部802中保存的全部转换密文RC和由输入部803输入的第2公开密钥epk生成密文EC。虽然未图示，但是，为了生成密文EC，同态运算部804也可以具有随机数生成功能等。发送部805输出密文EC。

[0093] 图9是示出第1解密装置900的结构的框图。如图9所示，第1解密装置900具有接收部901、保管部902、输入部903、解密处理部904和发送部905。虽然未图示，但是，第1解密装置900具有存储在第1解密装置900的各部中使用的数据的记录介质。接收部901输入解密密钥sk。保管部902保管由接收部901接收到的解密密钥sk。对输入部903输入密文C(D、E)、公开密钥pk。解密处理部904根据保管部902中保存的解密密钥sk和由输入部903输入的密文C生成密文C的解密结果M。发送部905输出解密结果M。

[0094] 图10是示出第2解密装置1000的结构的框图。如图10所示，第2解密装置1000具有接收部1001、保管部1002、输入部1003、解密处理部1004和发送部1005。虽然未图示，但是，第2解密装置1000具有存储在第2解密装置1000的各部中使用的数据的记录介质。接收部1001输入第2解密密钥esk。保管部1002保管由接收部1001接收到的第2解密密钥esk。输入部1003输入密文EC。解密处理部1004根据保管部1002中保存的第2解密密钥esk和由输入部1003输入的密文EC生成密文EC的解密结果EM。发送部1005输出解密结果EM。

[0095] 下面，对与本实施方式的各装置的计算方法相当的各装置的动作进行说明。

[0096] 还参照图20进行说明。图20是示出隐匿分析系统100的数据的输入和输出的图。

[0097] 图11是示出共享参数生成装置200的动作的流程图。如图20所示，共享参数生成装置200接收密钥的比特长度L_{bit}，生成共享参数pub，输出共享参数pub。

[0098] 在步骤S201中，输入部201接收密钥的比特长度L_{bit}。

[0099] 在步骤S202中，共享参数生成部202根据密钥的比特长度L_{bit}，生成能够进行配对运算的要素$BG=(p、G、G_T、e)$。

[0100] 这里，p表示群G和群G_T的位数。

[0101] e设具有$G\times G\rightarrow G_T$的映射的双线性映射。双线性映射是针对全部$g\in G$和$a、b\in Z_p$成为$e(g^a、g^b)=e(g、g)^{ab}\in G_T$的映射。将使用该e的运算称作配对运算。另外，$Z_p$是mod＝p的整数的集合。

[0102] 在步骤S203中，共享参数生成部202生成哈希函数H和哈希函数密钥k。

[0103] 在步骤S204中，共享参数生成部202从群G中随机选择g，随机选择$u、v、w\in Z_p$。

[0104] 在步骤S205中，共享参数生成部202计算$U=g^u、V=g^v、W=g^w、P=e(g、g)$，生成共享参数$pub=(BG、g、U、V、W、P、k)$。

[0105] 在步骤S206中，发送部203输出共享参数pub。

[0106] 另外，发送部203是输出部，如图1所示，假设经由互联网101进行发送，但是，也可以向内置存储介质或已安装的存储介质输出共享参数pub。这对于后述全部发送部也是同样的。

[0107] 图12是示出第1密钥生成装置300的动作的流程图。如图20所示，第1密钥生成装置300接收共享参数pub，使用共享参数pub生成第1公开密钥pk、第1解密密钥sk，输出第1公开密钥pk、第1解密密钥sk。

[0108] 在步骤S301中，输入部301接收共享参数pub。

[0109] 在步骤S302中，密钥生成部302随机选择解密密钥$sk\in Z_p$。

[0110] 在步骤S303中，密钥生成部302计算公开密钥$pk=g^{sk}$。

[0111] 在步骤S304中，密钥发送部303发送公开密钥pk和解密密钥sk。

[0112] 图13是示出第2密钥生成装置400的动作的流程图。如图20所示，第2密钥生成装置

400接收共享参数pub，使用共享参数pub生成第2公开密钥epk、第2解密密钥esk，输出第2公开密钥epk、第2解密密钥esk。在转换密钥rk的生成、密文RC到密文EC的加密中使用第2公开密钥epk。在密文EC的解密中使用第2解密密钥esk。

[0113] 在步骤S401中，输入部401接收共享参数pub。

[0114] 在步骤S402中，密钥生成部402使用共享参数pub，随机选择解密密钥$esk \in Z_p$。

[0115] 在步骤S403中，密钥生成部402计算公开密钥$epk = g^{esk}$。

[0116] 在步骤S404中，密钥发送部403发送第2公开密钥epk和第2解密密钥esk。

[0117] 图14是示出加密装置500的动作的流程图。根据图14对加密装置500的加密方法进行说明。如图20所示，加密装置500接收共享参数pub、公开密钥pk。并且，加密装置500取得明文M。加密装置500生成并输出密文C。

[0118] 在步骤S501中，接收部501接收共享参数pub、公开密钥pk。保管部502保管共享参数pub、公开密钥pk。

[0119] 输入部503接收明文M。

[0120] 在步骤S502中，加密部504使用共享参数pub，随机选择随机数$r、s \in Z_p$。

[0121] 在步骤S503中，加密部504使用成对的2个密钥中的一个密钥即第1公开密钥pk对明文M进行加密，由此，生成对明文M进行加密后的能够进行同态运算的密文D。

[0122] 具体而言，加密部504计算下式作为密文D。

[0123] $C_0 = M \cdot P^r$ (式1)

[0124] $C_1 = pk^r$ (式2)

[0125] $D = (C_0、C_1)$。这里，“·”表示群G内定义的乘法运算。

[0126] 在式1、式2中，M是明文。

[0127] P是共享参数pub中包含的配对运算P。

[0128] 随机数r是在S502中选择出的。

[0129] pk是第1公开密钥pk。

[0130] 这样，加密部504选择第1随机数r和第2随机数s，除了第1公开密钥pk以外，还使用第1随机数r和共享参数pub生成密文D。

[0131] 并且，检测要素生成部505使用第1公开密钥pk和密文$D = (C_0、C_1)$，生成在密文D的改变检测中使用的检测要素E。

[0132] 具体而言，检测要素生成部505计算下式。

[0133] $t = H(k、(pk、C_0、C_1))$ (式3)

[0134] $C_2 = (U^s V^t W)^r$ (式4)

[0135] 在(式3)(式4)中，式3右边的$H(k、(pk、C_0、C_1))$表示通过哈希函数H、哈希密钥k对$(pk、C_0、C_1)$进行加密。哈希函数H、哈希密钥k的信息包含在共享参数pub中。式4右边的U、V、W包含在共享参数pub中。t是通过式3得到的，随机数r、随机数s是S502的随机数。随机数r记作第1随机数，随机数s记作第2随机数。如式3、式4所示，除了第1公开密钥pk和密文D以外，检测要素生成部505还使用第1随机数r、第2随机数s和共享参数pub生成检测要素E。

[0136] 在步骤S504中，发送部506输出$C = (C_0、C_1、s、C_2)$。

[0137] $C = (C_0、C_1、s、C_2) = (D、E)$。这里，$C_0、C_1$相当于密文D，$C_2$相当于检测要素E。

[0138] 作为输出部的发送部506输出密文D和检测要素E。

[0139] 图15是示出转换密钥生成装置600的动作的流程图。如图20所示，转换密钥生成装置600接收共享参数pub、第1解密密钥sk和第2公开密钥epk，生成并输出转换密钥rk。

[0140] 在步骤S601中，接收部601接收解密密钥sk，保管部602保管解密密钥sk。输入部603接收第2公开密钥epk。

[0141] 在步骤S602中，转换密钥生成部604计算$rk=epk^{1/sk}$。根据与在对密文D实施了同态运算的情况下在同态运算的运算结果的解密中使用的第2秘密密钥esk(第2解密密钥)成对的第2公开密钥epk和第1解密密钥sk(第1秘密密钥)，生成转换密钥rk。

[0142] 在步骤S603中，发送部605输出转换密钥rk。

[0143] 图16是示出密文转换装置700的动作的流程图。使用图16对密文转换装置700的密文转换方法进行说明。如图20所示，密文转换装置700接收共享参数pub、第1公开密钥pk、转换密钥rk、$C=(D、E)=(C_0、C_1、s、C_2)$，将密文C转换成密文RC，输出密文RC。

[0144] 在步骤S701中，接收部701接收转换密钥rk。保管部702保管转换密钥rk、共享参数pub、第1公开密钥pk等。在向作为与密文D不同的密文的转换密文RC的转换中使用转换密钥rk。输入部703接收密文$C=(D、E)$和第1公开密钥pk。密文C包含对明文M进行加密后的密文D和检测要素E。密文D能够进行同态运算。这样，作为取得部的输入部703取得对明文M进行加密后的能够进行同态运算的密文D和在密文D的改变检测中使用的检测要素E。

[0145] 在步骤S702中，改变检测部704计算$t'=H(k、(pk、C_0、C_1))$。

[0146] $t'=H(k、(pk、C_0、C_1))$意味着使用哈希函数H和哈希密钥k对$(pk、C_0、C_1)$进行加密。C_0、C_1包含在密文C中。

[0147] 在步骤S703中，改变检测部704验证$e(C_2、pk)=e(C_1、(U^sV^{t'}W))$是否成立。在成立的情况下即未检测到改变的情况下，处理进入步骤S705，在不成立的情况下即检测到改变的情况下，处理进入步骤S704。

[0148] 这样，改变检测部704根据作为检测要素E的C_2生成作为密文D是否被改变的基准的基准值的$e(C_2、pk)$，根据密文D生成在与基准值之间的核对中使用的核对值的$e(C_1、(U^sV^{t'}W))$。核对值的$e(C_1、(U^sV^{t'}W))$包含$t'=H(k、(pk、C_0、C_1))$。

[0149] 在t'中，C_0、C_1是密文D。

[0150] 由此，根据密文D生成核对值的$e(C_1、(U^sV^{t'}W))$。

[0151] 改变检测部704进行基准值与核对值之间的核对。

[0152] 更具体而言，改变检测部704根据检测要素E和第1公开密钥pk生成基准值的$e(C_2、pk)$，根据第1公开密钥pk和密文D生成核对值的$e(C_1、(U^sV^{t'}W))$。

[0153] 在步骤S704中，密文转换部705为$RC=\perp$。

[0154] $\perp$是表示转换失败的特殊符号，只要规定表示密文转换失败即可，可以是任意记号。

[0155] 在步骤S705中，密文转换部705计算$C'_1=e(C_1、rk)=e(pk^r、rk)$，生成转换密文$RC=(C_0、C'_1)=(M\cdot P^r、e(pk^r、rk))$。这样，作为转换部的密文转换部705在改变检测部704的核对结果为未检测到密文D的改变的情况下，通过使用转换密钥rk，将密文D转换成从密文D转换而成的转换密文RC。

[0156] 在步骤S706中，作为输出部的发送部706输出转换密文$RC=(C_0、C'_1)$。

[0157] 图17是示出同态运算装置800的动作的流程图。如图20所示，同态运算装置800接

收共享参数pub、第2公开密钥epk、多个(n个)RC。将n个RC分别记作RC^i。

[0158] 在步骤S801中，接收部801接收转换后的密文RC，保管部802保管密文RC。然后，输入部803接收第2公开密钥epk。

[0159] 在步骤S802中，同态运算部804选择随机数$r' \in Z_p$。

[0160] 在步骤S803中，同态运算部804利用以下式子新计算左边的C_0、C'_1。

[0161] 以下式子假设存在利用以下式子得到的同态运算结果的请求。同态运算部804响应于该请求，进行以下式子的运算。

[0162] 计算$C_0 = P^{r'} \Pi_{i\in[n]} C^i{}_0$、$C'_1 = e(g, epk)^{r'} \times \Pi_{i\in[n]} C'^i{}_1$。

[0163] 在步骤S804中，发送部805输出上述同态运算后的密文EC即$EC = (C_0, C'_1)$。

[0164] 图18是示出第1解密装置900的动作的流程图。

[0165] 如图20所示，第1解密装置900接收共享参数pub、第1公开密钥pk、第1解密密钥sk、密文$C = (C_0, C_1, s, C_2)$。第1解密装置900将密文C解密成明文M。

[0166] 在步骤S901中，接收部901接收共享参数pub、第1公开密钥pk、第1解密密钥sk。保管部902保管共享参数pub、第1公开密钥pk、第1解密密钥sk。输入部903接收密文C。

[0167] 在步骤S902中，解密处理部904计算$t' = H(k, (pk, C_0, C_1))$。

[0168] 在步骤S903中，解密处理部904验证$e(C_2, pk) = e(C_1, (U^s V^{t'} W))$是否成立，在成立的情况下进入步骤S905，在不成立的情况下进入步骤S904。

[0169] 在步骤S904中，解密处理部904为$M = \perp$。$\perp$是表示转换失败的特殊符号，只要规定表示密文转换失败即可，可以是任意记号。

[0170] 在步骤S905中，解密处理部904计算$M = C_0 / e(C_1, g)^{1/sk}$。

[0171] 在步骤S906中，发送部905输出解密结果M。

[0172] 图19是示出第2解密装置1000的动作的流程图。如图20所示，第2解密装置1000接收共享参数pub、第2秘密密钥esk、密文$EC = (C_0, C'_1)$。第2解密装置1000对密文EC进行解密，输出解密结果EM。

[0173] 在步骤S1001中，接收部1001接收第2解密密钥esk，保管部1002保管第2解密密钥esk。输入部1003接收同态运算后的密文EC。

[0174] 在步骤S1002中，解密处理部1004计算$EM = C_0 / (C'_1)^{1/esk}$。

[0175] 在步骤S1003中，发送部1005输出解密结果EM。

[0176] <***实施方式1的效果的说明***>

[0177] 本实施方式发挥以下效果。

[0178] (1)在本实施方式中，即使是利用不同的公开密钥加密后的数据，通过使用转换密钥，也能够转换成相同的第2公开密钥epk的密文。由此，通过使用同态运算装置，能够在隐匿了各个密文的信息的状态下执行明文的运算。

[0179] (2)在本实施方式中，关于密文C，在解密装置的解密处理中确认使用t的验证式，因此，无法对密文C内的明文M进行变更。但是，通过使用转换密钥，能够转换成相同的第2公开密钥epk的密文，因此，通过使用同态运算装置，能够在隐匿了各个密文的信息的状态下执行明文的运算。

[0180] (3)在本实施方式中，使用公开密钥pk的密文C的安全性非常高，但是，能够在隐匿的状态下进行明文M的运算，因此，能够实现安全的隐匿分析巢统。

[0181] (4)加密装置在密文C中包含密文D和检测密文D的改变的检测要素E，因此，能够防止密文D的改变。

[0182] (5)密文转换装置使用检测要素E验证密文D有无改变后，在判断为没有改变的情况下，将密文C转换成密文RC。由此，能够对同态运算装置提供未被改变的密文C。

[0183] ***其他结构***

[0184] 并且，在本实施方式中，作为处理器91示出的“部”的功能通过软件实现，但是，作为变形例，作为处理器91示出的“部”的功能也可以通过硬件实现。

[0185] 图22示出作为处理器91示出的“部”的功能通过作为硬件的处理电路99实现的情况。处理电路99与信号线99a连接。通过处理电路99实现所述作为处理器91示出的“部”的功能和“保管部”的功能。处理电路99是实现作为处理器91示出的“部”的功能和“保管部”的功能的专用电子电路。具体而言，处理电路99是单一电路、复合电路、程序化的处理器、并列程序化的处理器、逻辑IC、GA(Gate Array:门阵列)、ASIC(Application Specific Integrated Circuit:面向特定用途的集成电路)或FPGA(Field-Programmable Gate Array:现场可编程门阵列)。

[0186] 作为处理器91示出的“部”的功能可以由一个处理电路99实现，也可以分散在多个处理电路99中实现。

[0187] 作为另一个变形例，图2～图10所示的装置也可以由软件和硬件的组合来实现。即，也可以是，图2～图10所示的装置的一部分功能由专用硬件实现，其余功能由软件实现。

[0188] 将处理器91、存储装置92和处理电路99统称作“处理电路系统”。即，图2～图10中的作为处理器91示出的“部”的功能和“保管部”由处理电路系统实现。

[0189] 可以将作为处理器91示出的“部”改写成“工序”或“步骤”或“处理”。并且，也可以利用固件实现作为处理器91示出的“部”的功能。

[0190] 并且，图2～图10所示的共享参数生成装置200～第2解密装置1000的动作能够作为方法、程序来理解。加密装置500通过加密程序进行动作。加密装置500的动作是加密方法。并且，密文转换装置700通过密文转换程序进行动作。密文转换装置700的动作是密文转换方法。

[0191] 另外，在实施方式1中使用了公开密钥pk、解密密钥sk，但是，也可以使公开密钥pk和解密密钥的作用相反，在解密中使用公开密钥pk。这对于公开密钥epk、解密密钥esk也是同样的。

[0192] 标号说明

[0193] pub:共享参数;RC:密文;pk:第1公开密钥;sk:第1解密密钥;epk:第2公开密钥;esk:第2解密密钥;rk:转换密钥;91:处理器;92:存储装置;93:输入接口;94:输出接口;99:处理电路;99a:信号线;100:隐匿分析系统;101:互联网;200:共享参数生成装置;201:输入部;202:共享参数生成部;203:发送部;300:第1密钥生成装置;301:输入部;302:密钥生成部;303:密钥发送部;400:第2密钥生成装置;401:输入部;402:密钥生成部;403:密钥发送部;500:加密装置;501:接收部;502:保管部;503:输入部;504:加密部;505:检测要素生成部;506:发送部;600:转换密钥生成装置;601:接收部;602:保管部;603:输入部;604:转换密钥生成部;605:发送部;700:密文转换装置;701:接收部;702:保管部;703:输入部;704:改变检测部;705:密文转换部;706:发送部;800:同态运算装置;801:接收部;802:保管部;

803:输入部;804:同态运算部;805:发送部;900:第1解密装置;901:接收部;902:保管部;903:输入部;904:解密处理部;905:发送部;1000:第2解密装置;1001:接收部;1002:保管部;1003:输入部;1004:解密处理部;1005:发送部。

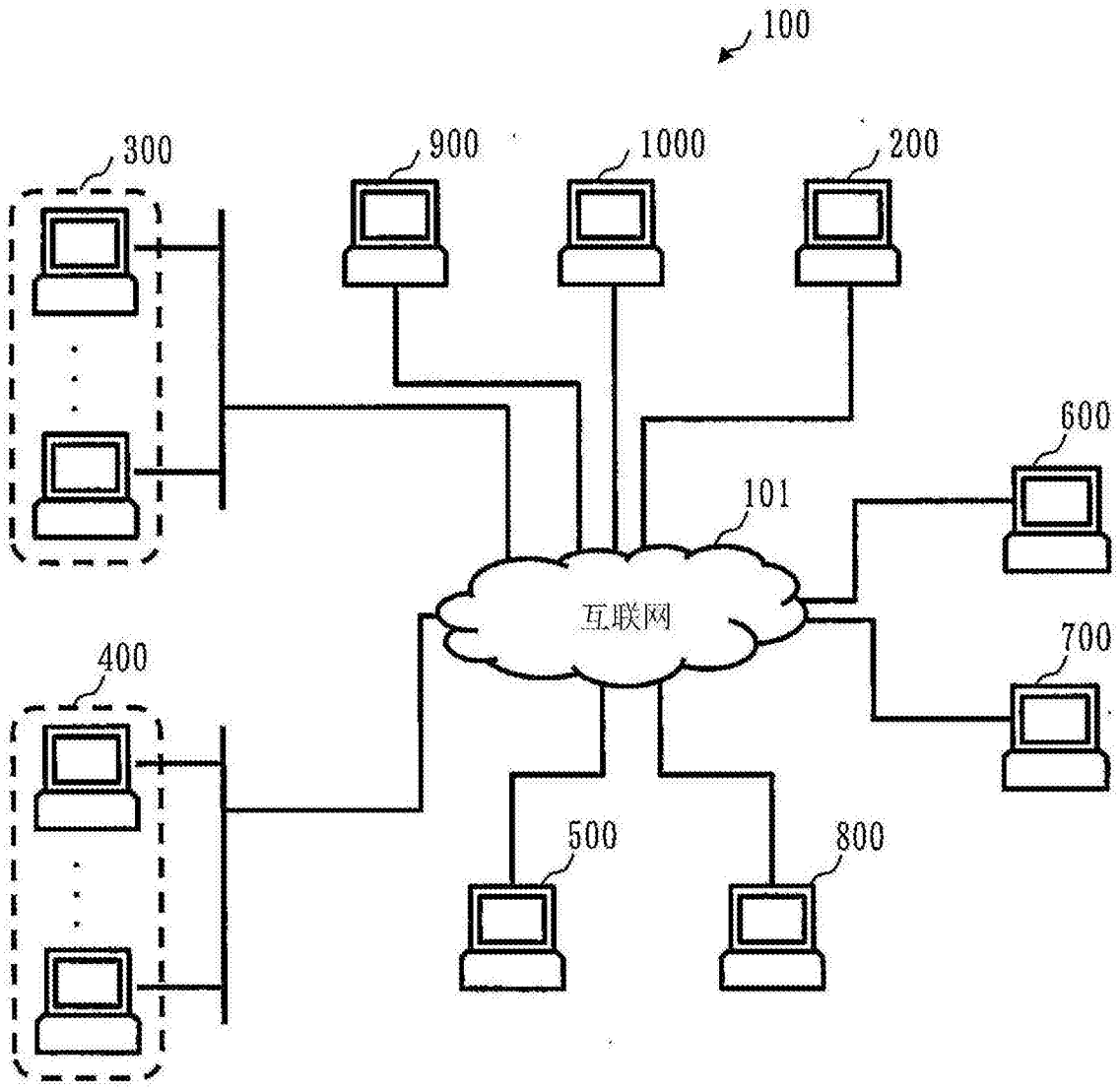


图1

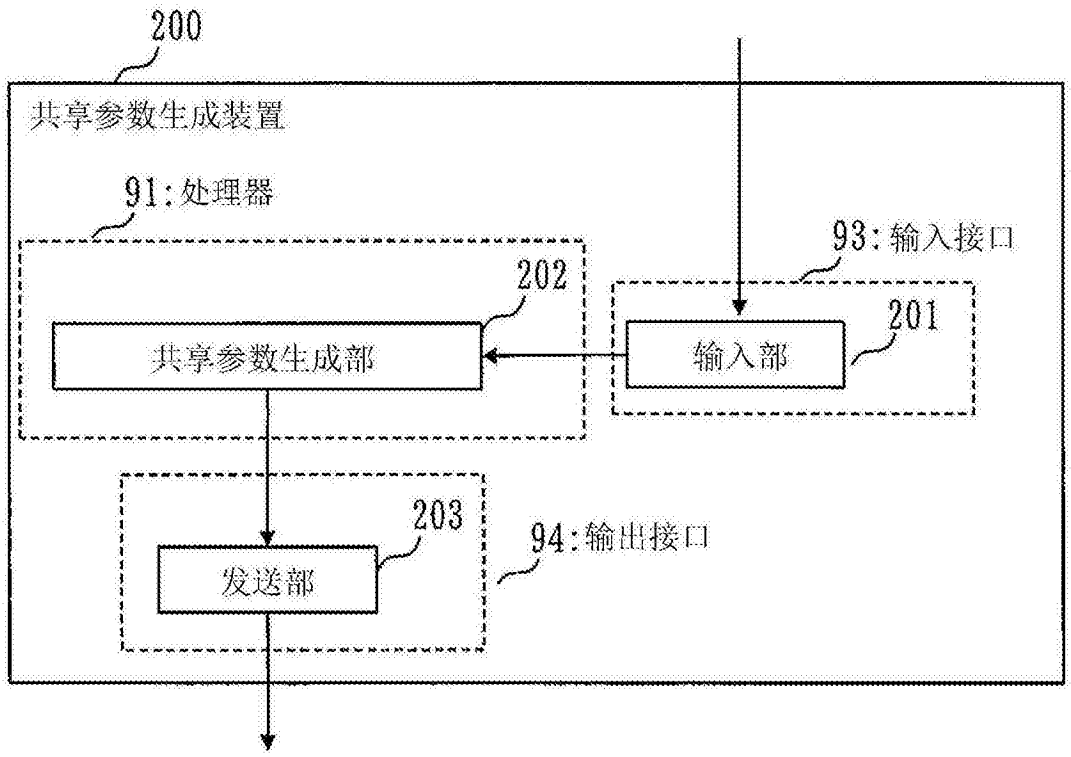

200
共享参数生成装置
91:处理器
93:输入接口
202
共享参数生成部
201
输入部
203
94:输出接口
发送部

图2

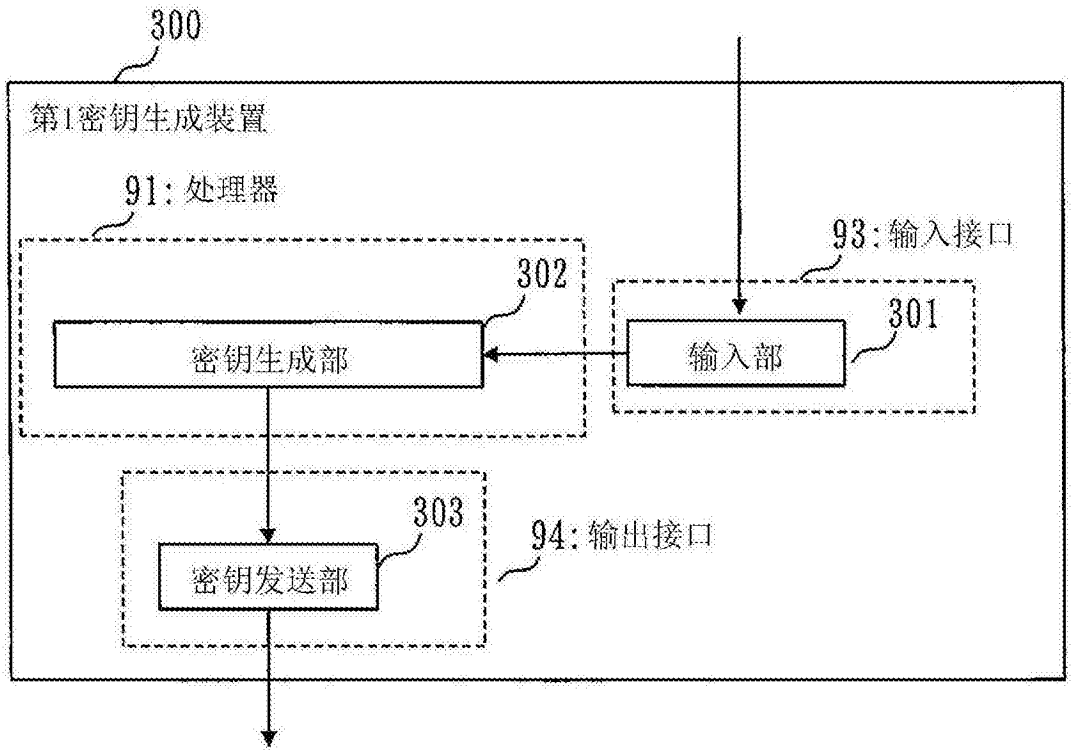

300
第1密钥生成装置
91:处理器
93:输入接口
302
密钥生成部
301
输入部
303
94:输出接口
密钥发送部

图3

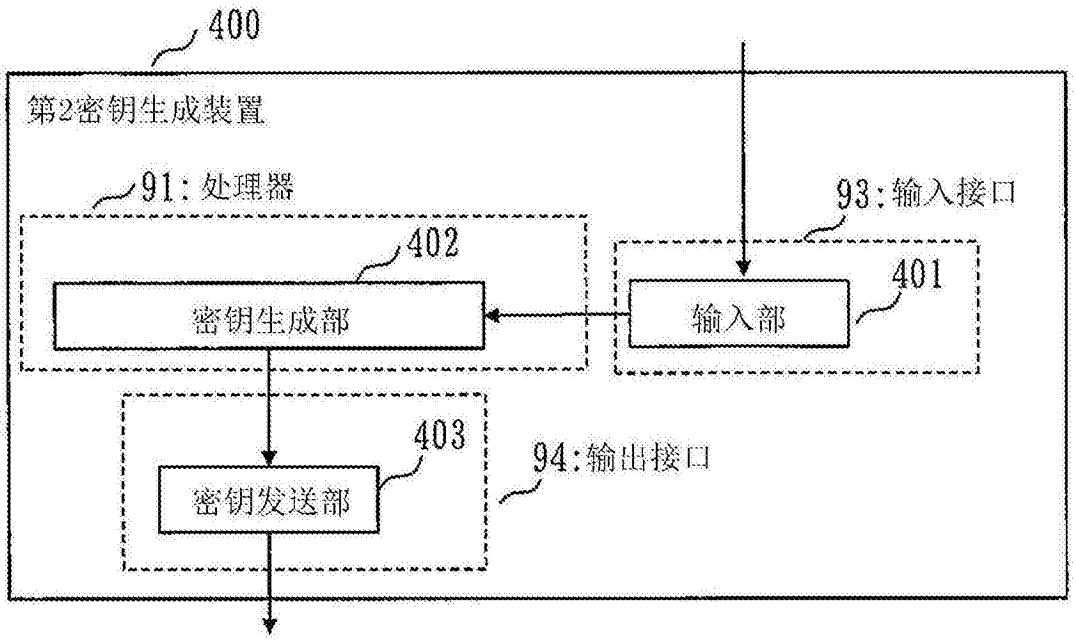

400
第2密钥生成装置
91:处理器
93:输入接口
402
密钥生成部
401
输入部
403
密钥发送部
94:输出接口

图4

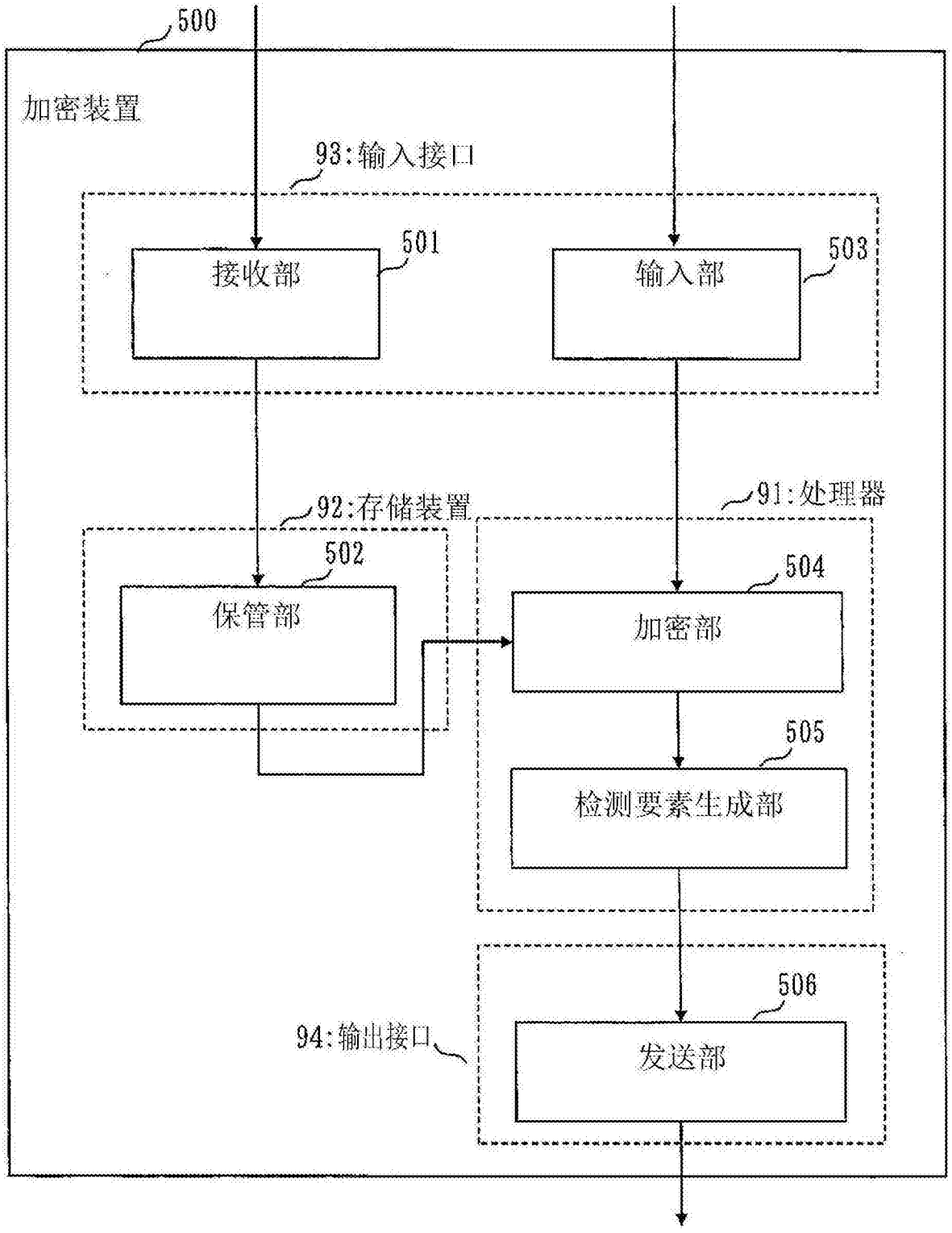

500
加密装置
93:输入接口
501
接收部
503
输入部
92:存储装置
91:处理器
502
保管部
504
加密部
505
检测要素生成部
506
94:输出接口
发送部

图5

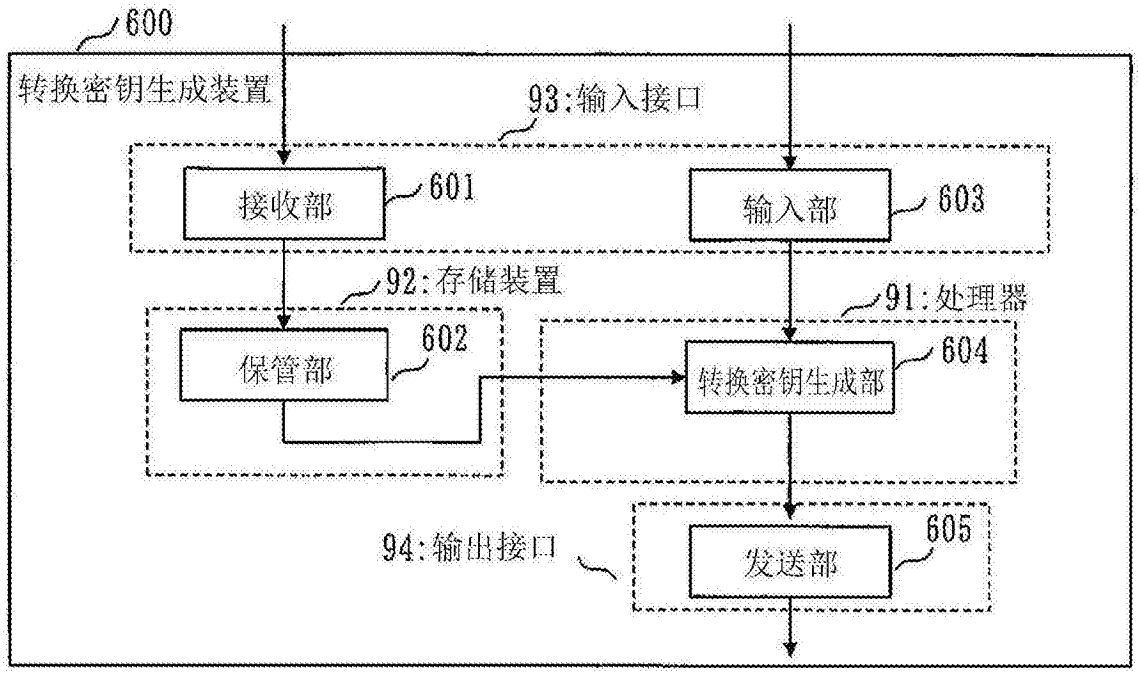

600
转换密钥生成装置
93:输入接口
接收部
601
输入部
603
92:存储装置
91:处理器
保管部
602
转换密钥生成部
604
94:输出接口
发送部
605

图6

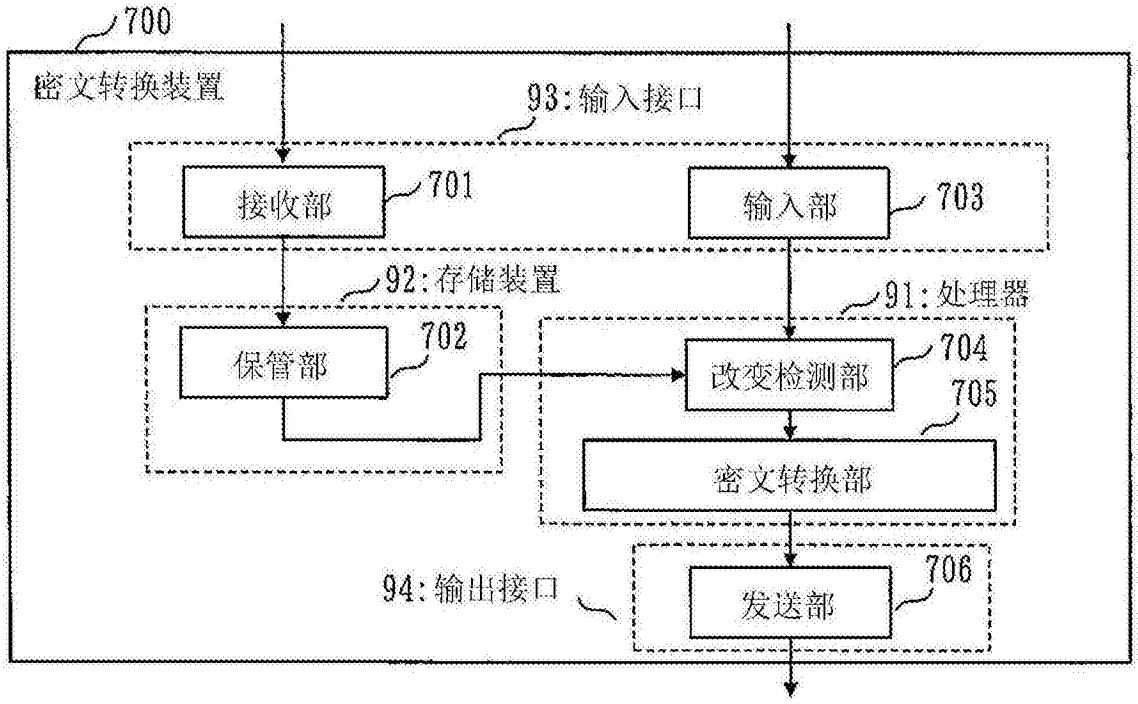

700
密文转换装置
93:输入接口
接收部
701
输入部
703
92:存储装置
91:处理器
保管部
702
改变检测部
704
705
密文转换部
94:输出接口
发送部
706

图7

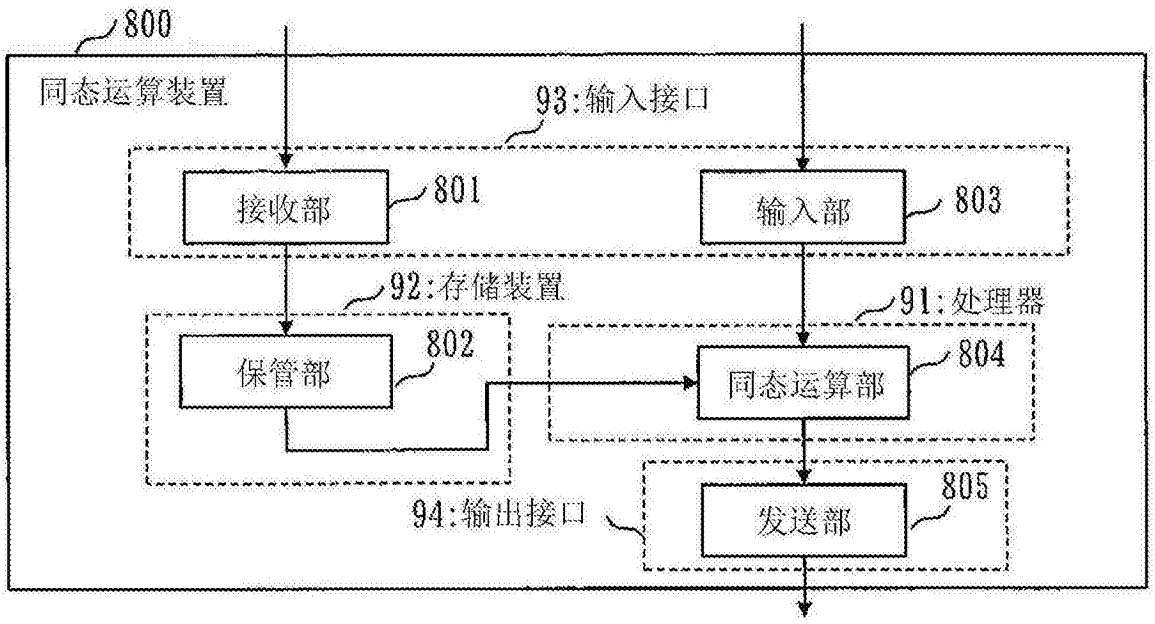

800
同态运算装置
93:输入接口
接收部
801
输入部
803
92:存储装置
91:处理器
保管部
802
同态运算部
804
94:输出接口
发送部
805

图8

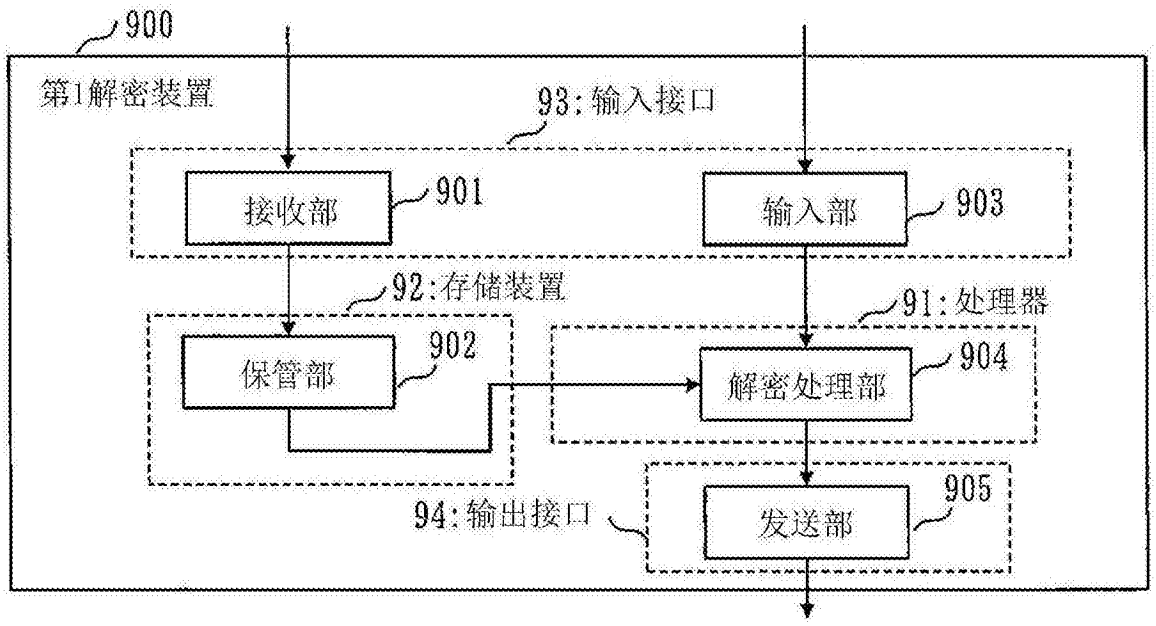

900
第1解密装置
93:输入接口
接收部
901
输入部
903
92:存储装置
91:处理器
保管部
902
解密处理部
904
94:输出接口
发送部
905

图9

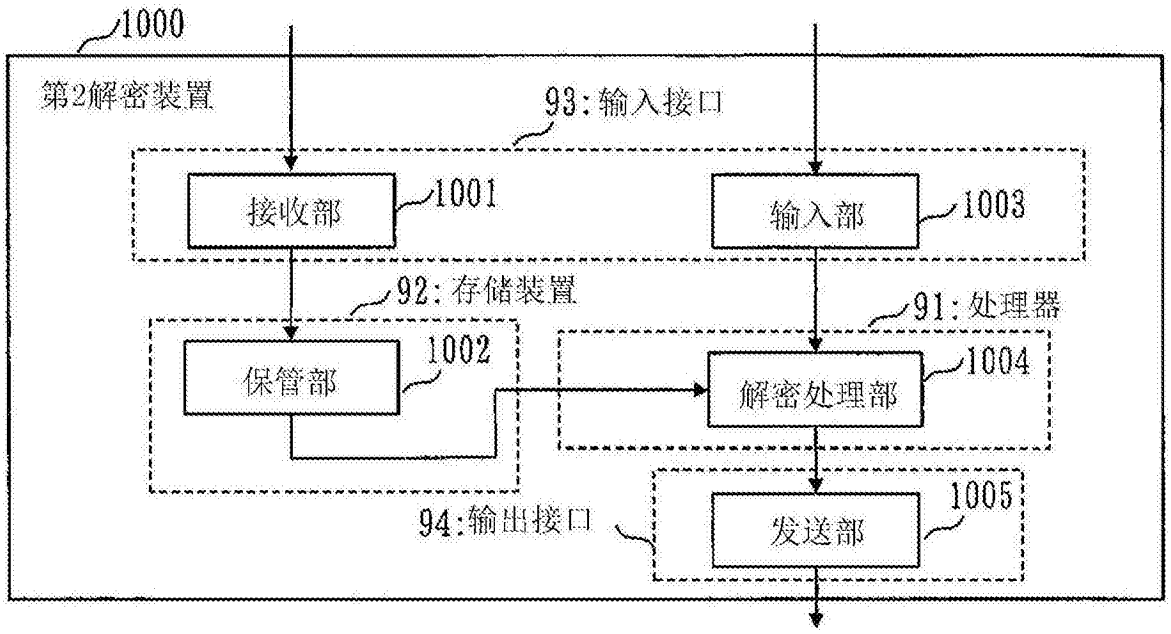

1000
第2解密装置
93:输入接口
接收部
1001
输入部
1003
92:存储装置
91:处理器
保管部
1002
解密处理部
1004
94:输出接口
发送部
1005

图10

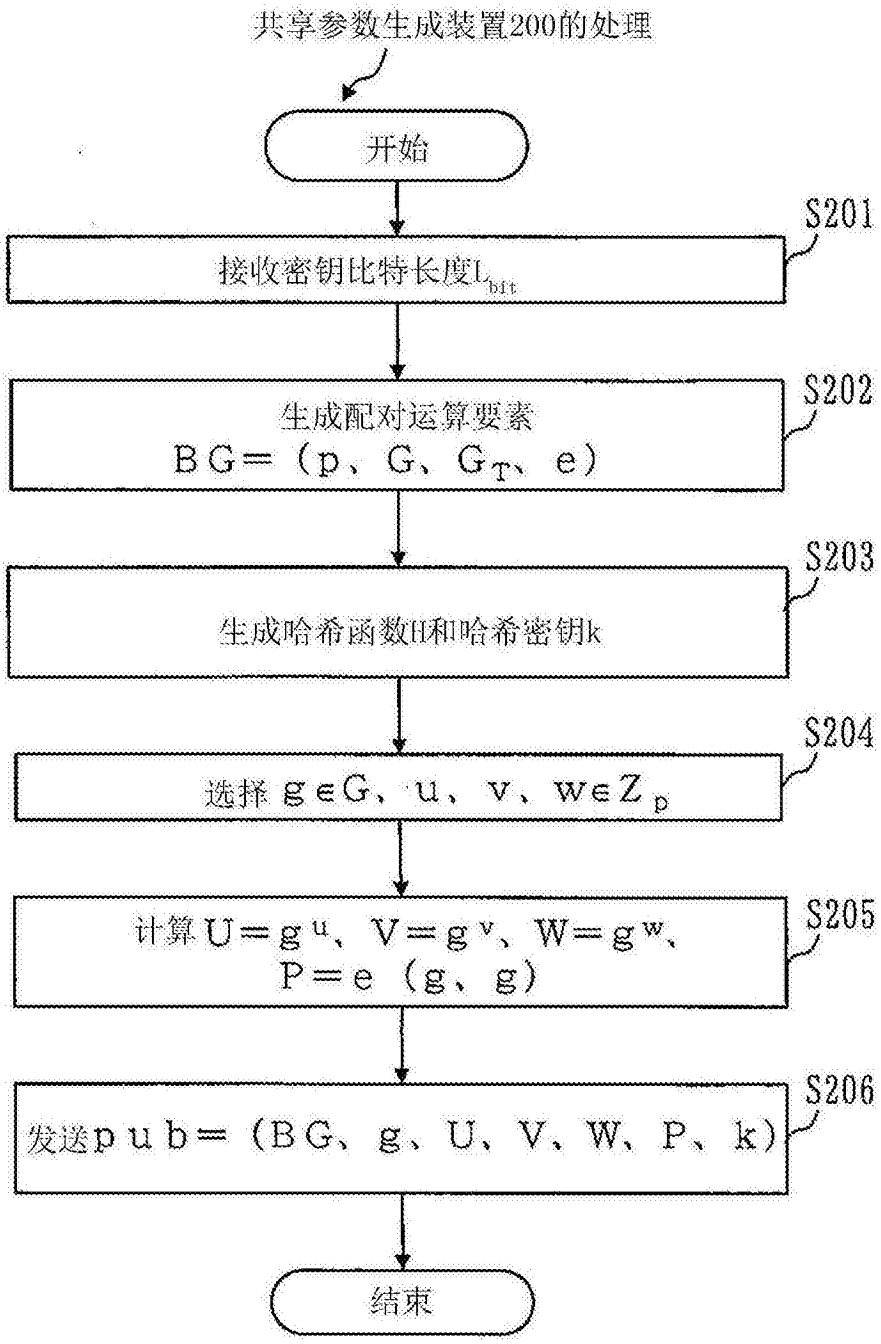

共享参数生成装置200的处理
开始
S201
接收密钥比特长度L_{bit}
S202
生成配对运算要素
BG=（p、G、G_T、e）
S203
生成哈希函数H和哈希密钥k
S204
选择 g∈G、u、v、w∈Z_p
S205
计算U=g^u、V=g^v、W=g^w、
P=e（g、g）
S206
发送pub=（BG、g、U、V、W、P、k）
结束

图11

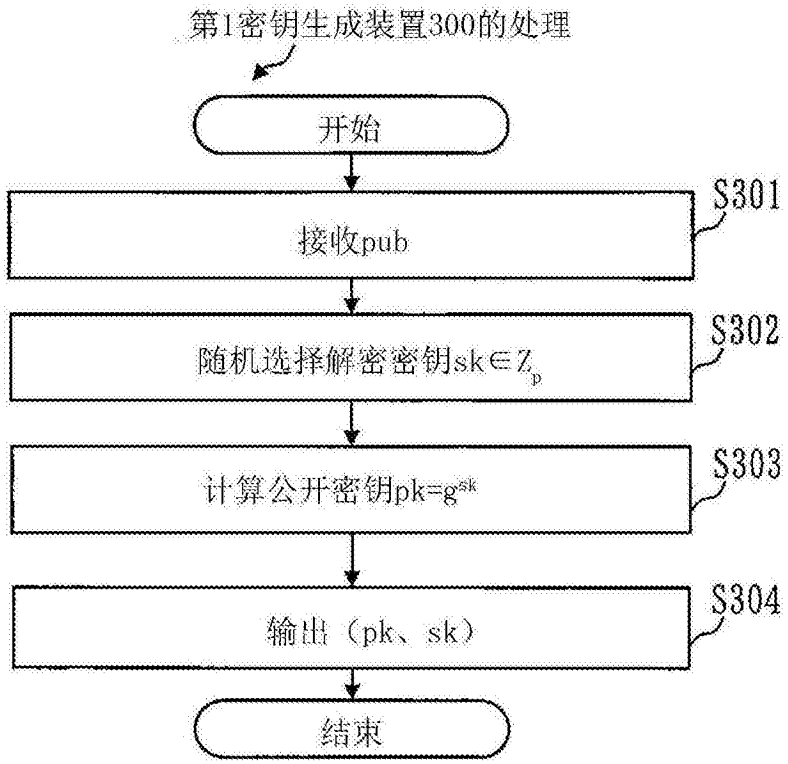

第1密钥生成装置300的处理
开始
接收pub
S301
随机选择解密密钥sk∈Zp
S302
计算公开密钥pk=g^sk
S303
输出（pk、sk）
S304
结束

图12

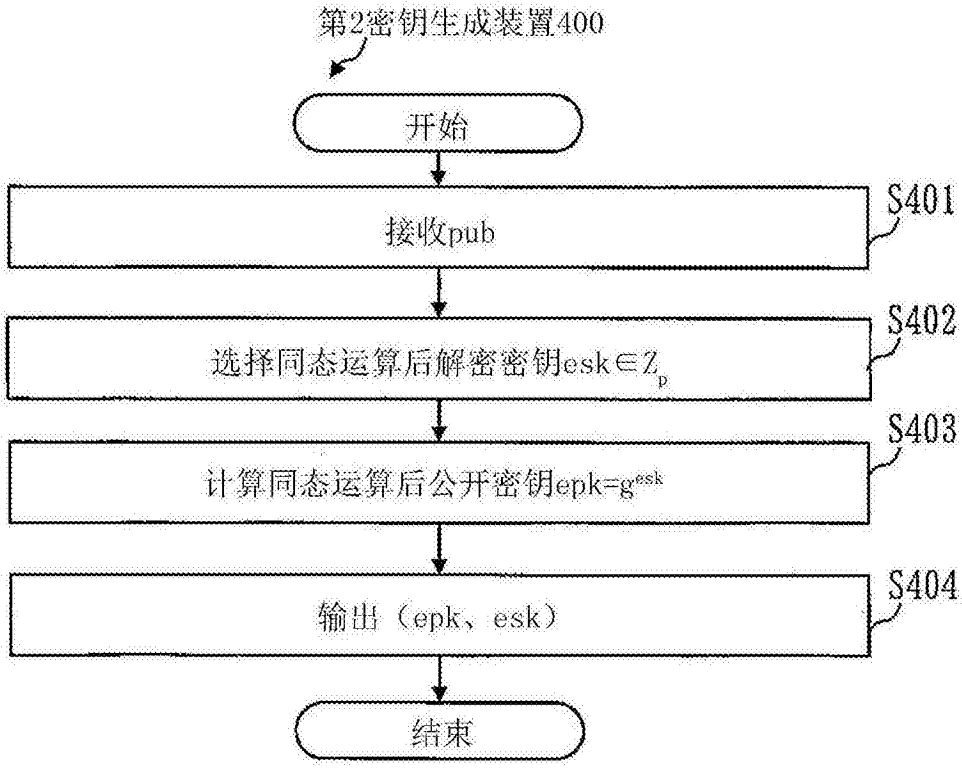

第2密钥生成装置400
开始
接收pub
S401
选择同态运算后解密密钥esk∈Zp
S402
计算同态运算后公开密钥epk=g^esk
S403
输出（epk、esk）
S404
结束

图13

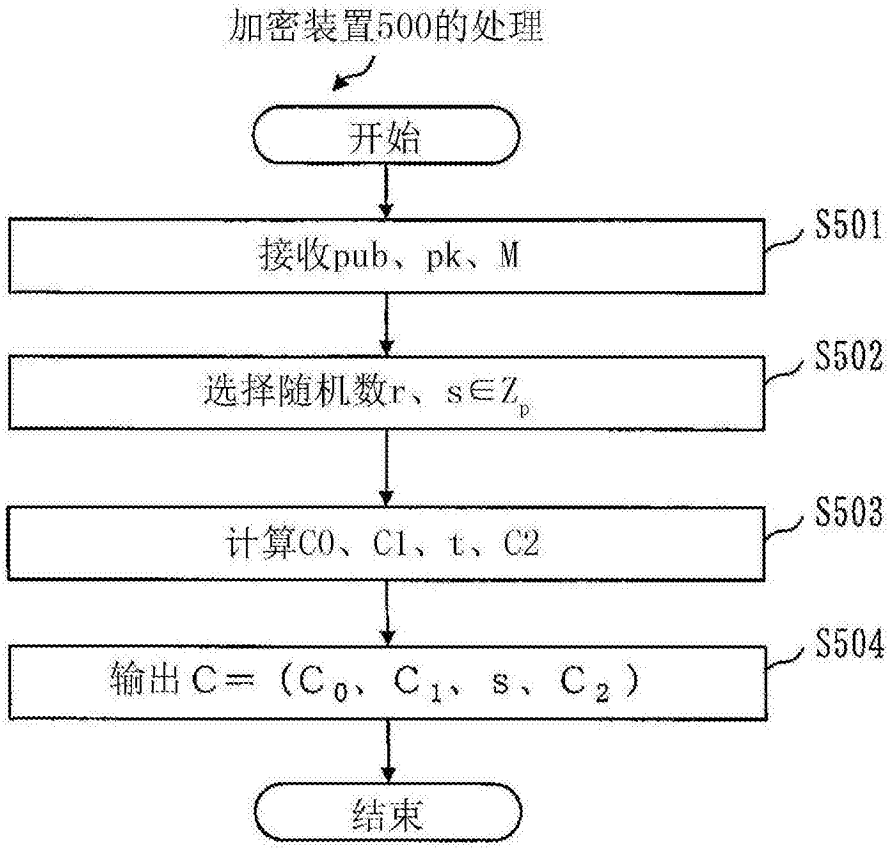

加密装置500的处理
开始
接收pub、pk、M
S501
选择随机数r、s∈Zp
S502
计算C0、C1、t、C2
S503
输出C=（C0、C1、s、C2）
S504
结束

图14

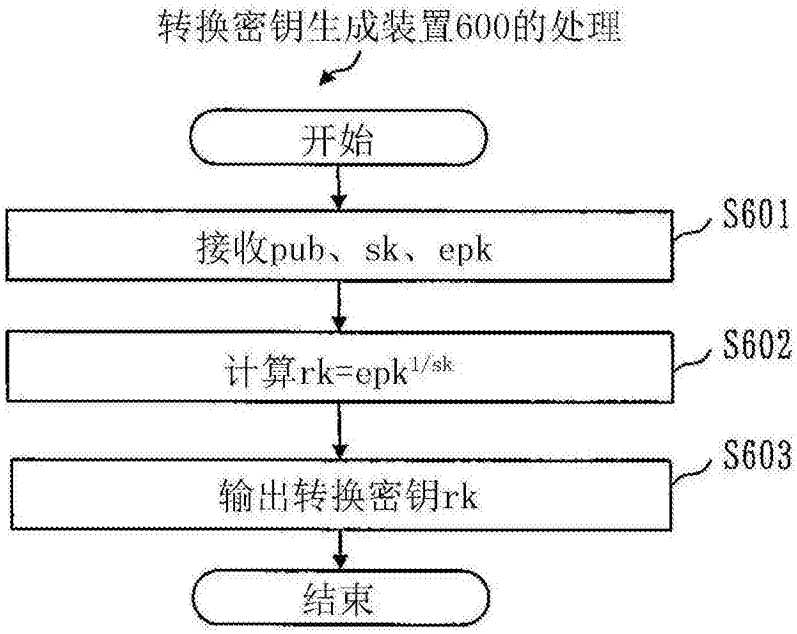

转换密钥生成装置600的处理
开始
接收pub、sk、epk
S601
计算rk=epk1/sk
S602
输出转换密钥rk
S603
结束

图15

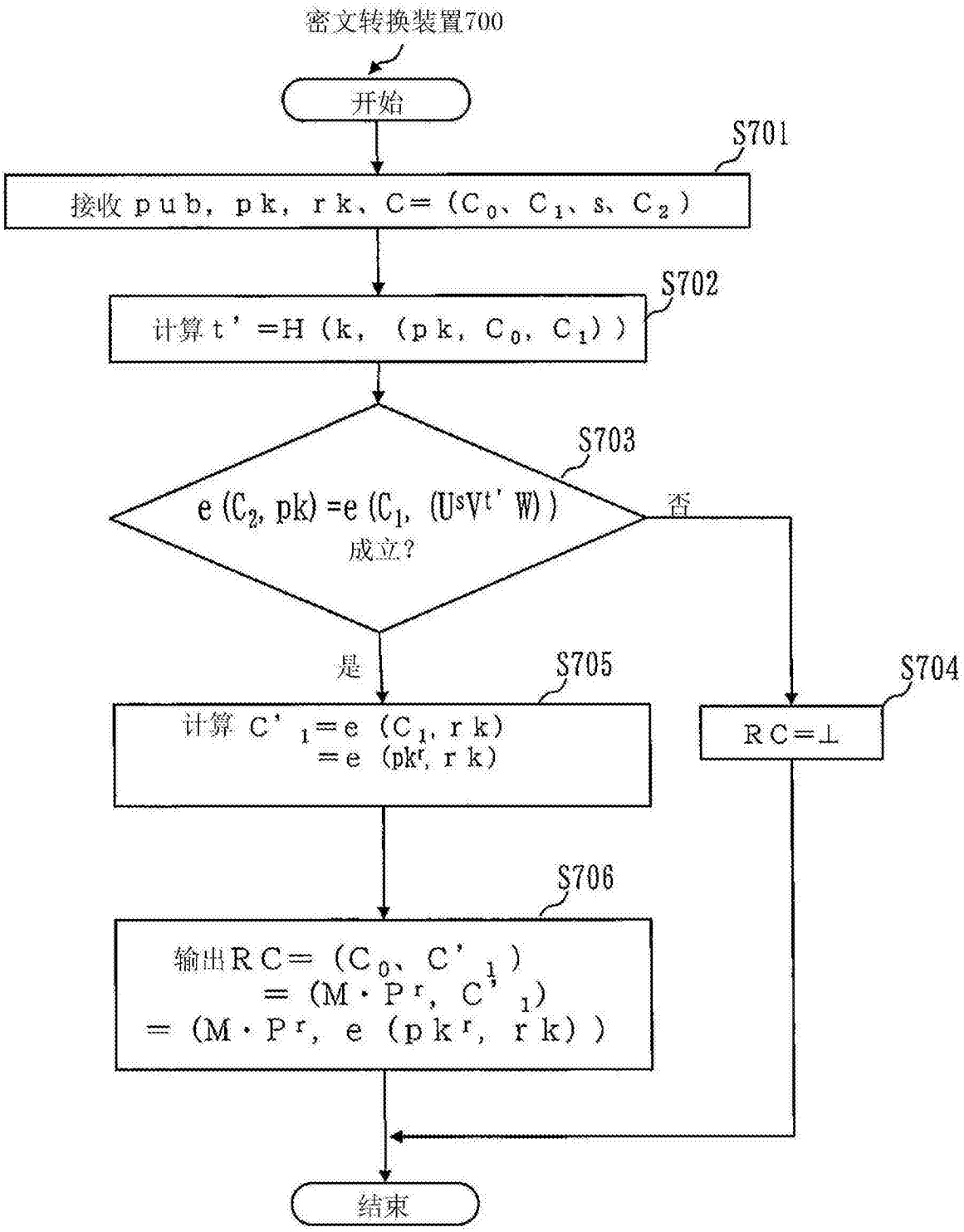

密文转换装置700
开始
S701
接收 pub, pk, rk, C=(C0、C1、s、C2)
S702
计算 t'=H(k, (pk, C0, C1))
S703
e(C2, pk)=e(C1, (UsVt' W))
成立?
否
是
S705
计算 C'1=e(C1, rk)
=e(pkr, rk)
S704
RC=⊥
S706
输出RC=(C0、C'1)
=(M·Pr, C'1)
=(M·Pr, e(pkr, rk))
结束

图16

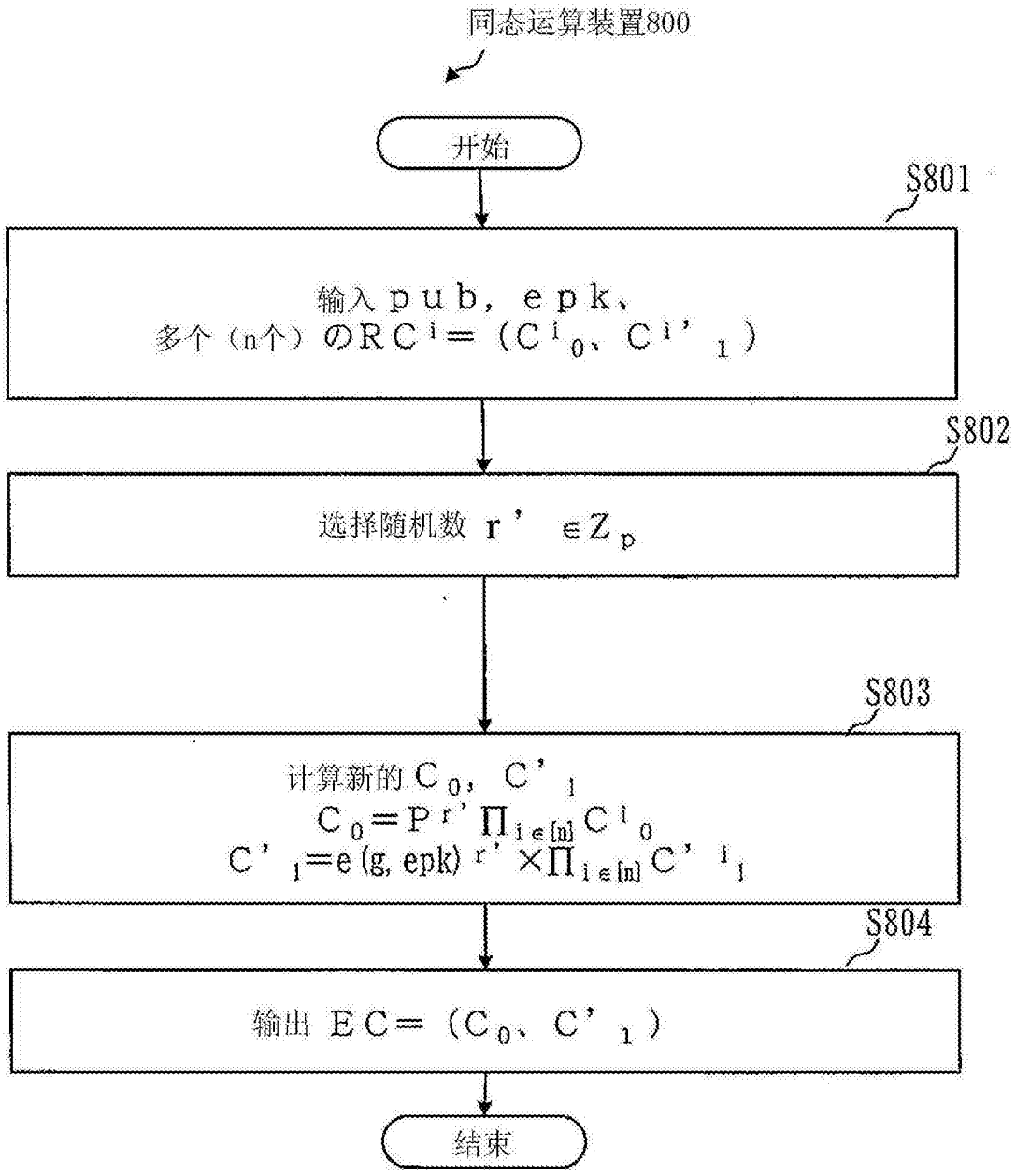

同态运算装置800
开始
S801
输入pub，epk、
多个（n个）のRC^i=（C^i_0、C^i'_1）
S802
选择随机数 r' ∈Z_p
S803
计算新的C_0，C'_1
C_0=P^r' ∏_{i∈[n]} C^i_0
C'_1=e(g, epk)^r' ×∏_{i∈[n]} C'^i_1
S804
输出 EC=（C_0、C'_1）
结束

图17

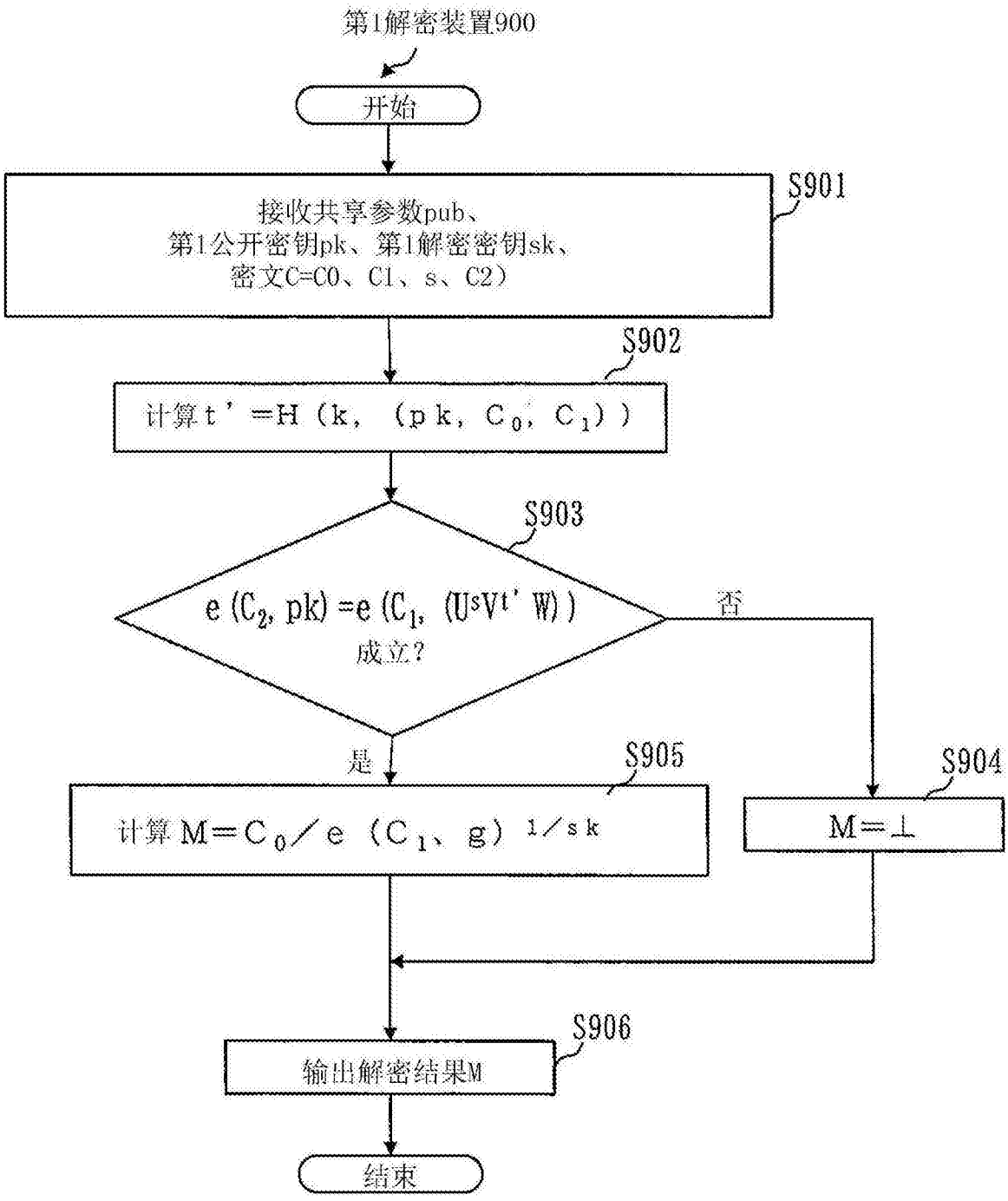

第1解密装置900
开始
S901
接收共享参数pub、
第1公开密钥pk、第1解密密钥sk、
密文C=C0、C1、s、C2）
S902
计算t'=H（k，（pk，C0，C1））
S903
e（C2，pk）=e（C1，（UsVt' W））
成立？
否
是
S905
计算M=C0／e（C1、g）1／sk
S904
M=⊥
S906
输出解密结果M
结束

图18

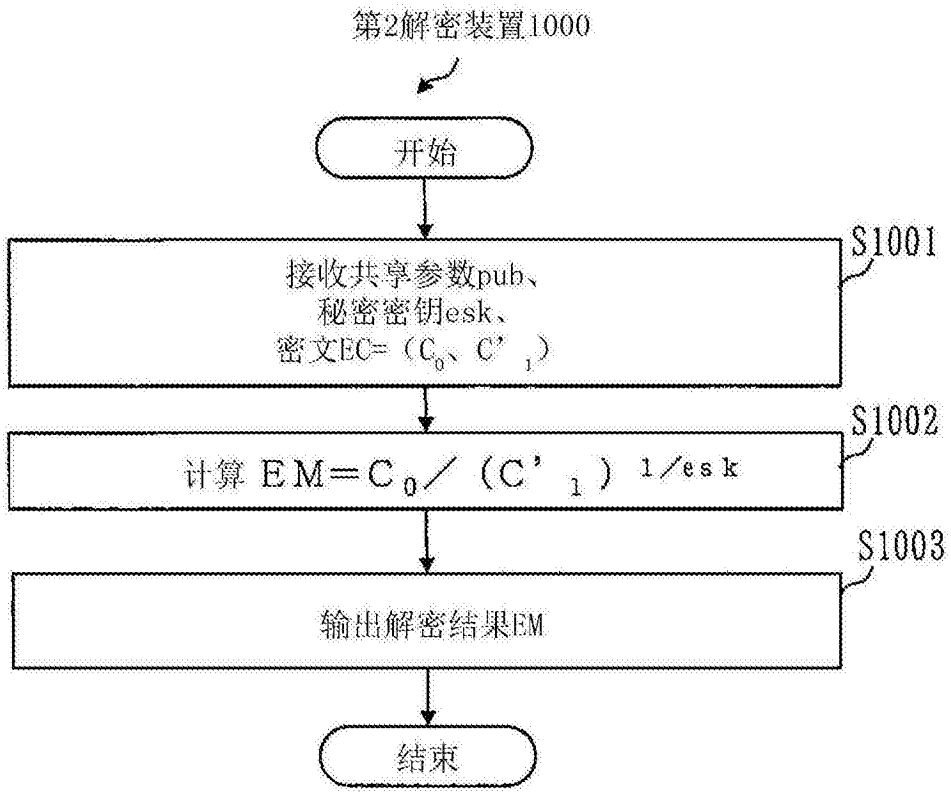

第2解密装置1000
开始
S1001
接收共享参数pub、
秘密密钥esk、
密文EC=（C0、C'1）
S1002
计算 EM=C0／（C'1）1/esk
S1003
输出解密结果EM
结束

图19

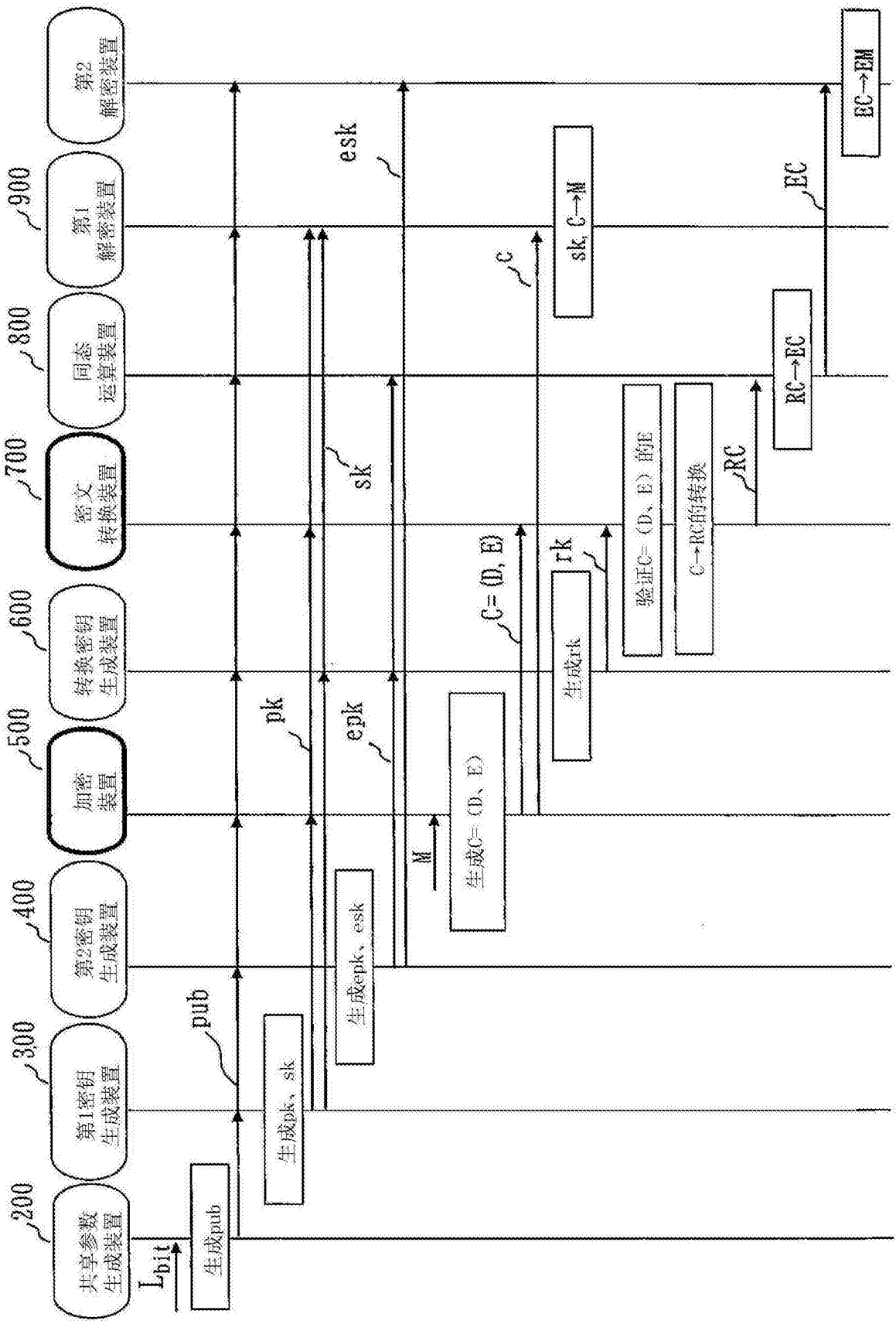

200
共享参数生成装置
300
第1密钥生成装置
400
第2密钥生成装置
500
加密装置
600
转换密钥生成装置
700
密文转换装置
800
同态运算装置
900
第1解密装置
第2解密装置
L_{bit}
生成pub
pub
生成pk、sk
pk
生成epk、esk
epk
esk
M
生成C=（D、E）
C=（D、E）
sk
生成rk
rk
c
sk, C→M
验证C=（D、E）的E
C→RC的转换
RC
RC→EC
EC
EC→EM

图20

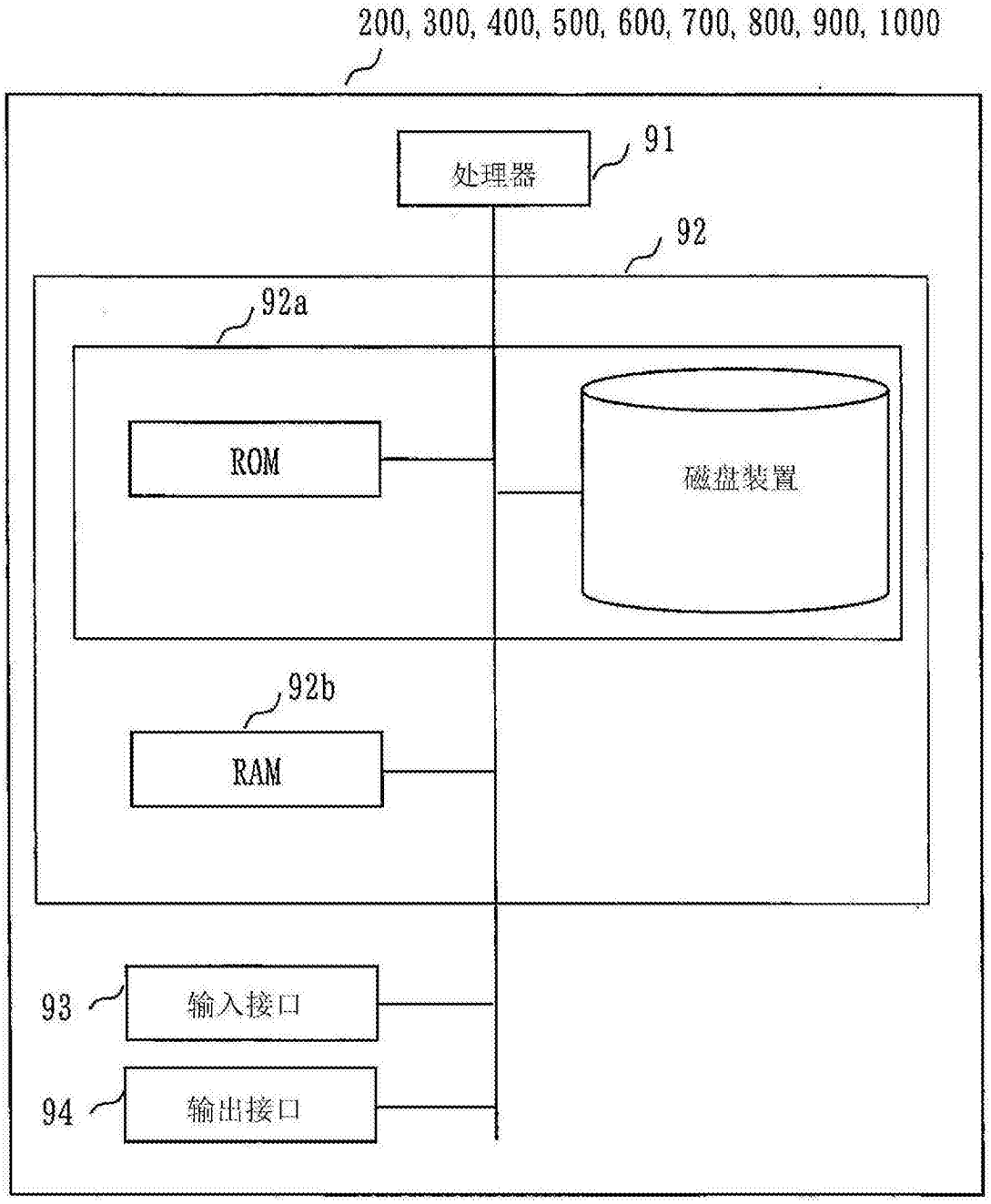

200, 300, 400, 500, 600, 700, 800, 900, 1000
处理器
91
92
92a
ROM
磁盘装置
92b
RAM
93
输入接口
94
输出接口

图21

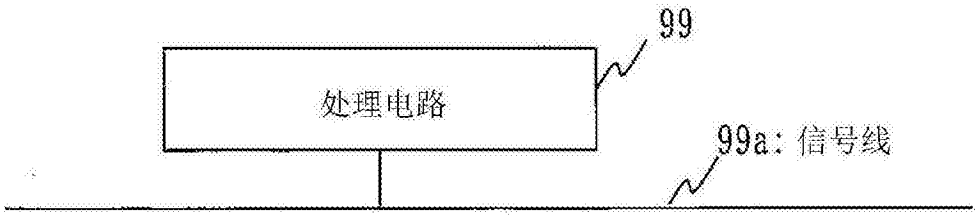

99
处理电路
99a: 信号线

图22